FORM-PTO-1390 (Rev. 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 032326-114

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5): 09/744652 Unassigned

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR99/01826	26 July 1999	27 July 1998

TITLE OF INVENTION
Method for Controlling the Execution of a Request for Action Transmitted by a Server to a Chip Card via a Terminal

APPLICANT(S) FOR DO/EO/US
Dominique DREHER and Patrick IMBERT

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

U.S. APPLICATION NO (If known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Unassigned 09/744652	PCT/FR9901826	032326-114

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,000.00 (960)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00 (970)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00 (958)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00 (956)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

Claims	Number Filed	Number Extra	Rate		
Total Claims	17-20 =	-0-	X$18.00 (966)	$ -0-	
Independent Claims	2-3 =	-0-	X$80.00 (964)	$ -0-	
Multiple dependent claim(s) (if applicable)			+$270.00 (968)	$ -0-	
TOTAL OF ABOVE CALCULATIONS =				$ 860.00	
Reduction for 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$ -0-	
SUBTOTAL =				$ 860.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$ -0-	
TOTAL NATIONAL FEE =				$ 860.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ -0-	
TOTAL FEES ENCLOSED =				$ 860.00	
				Amount to be: refunded	$
				charged	$

a. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Reg # 32,858
SIGNATURE

for James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

Patent
Attorney's Docket No. 032326-114

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Dominique DREHER et al	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: January 29, 2001	)	
	)	
For: METHOD FOR CONTROLLING THE EXECUTION OF A REQUEST FOR ACTION TRANSMITTED BY A SERVER TO A CHIP CARD VIA A TERMINAL	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title, insert the following:

--This disclosure is based upon, and claims priority from French Patent Application No. 98/09575, filed July 27, 1998, and International Application No. PCT/FR99/01826, filed July 26, 1999, the contents of which are incorporated herein by reference.

Background of the Invention--;

Page 2, line 5, delete "said".

Page 3, line 24, delete "said".

Page 4, before line 1, insert the following heading:

--**Summary of the Invention** --.

Page 6, between lines 25 and 26, insert the following heading:

--**Brief Description of the Drawings**--.

Page 7, between lines 7 and 8, insert the following heading:

--**Detailed Description**--.

Add the following Abstract:

--The invention concerns a method for exchanging synchronised messages between an application server and at least a chip card. The card transmits a message to the server containing the latest current value of an action counter stored by the server. The server sends a message comprising a request including one or several actions to be implemented by the card and stores the number of actions of the request. The card receives the message, successively executes the action or actions in the request, incrementing its action counter between each action when the action has been successfully executed. When there is a request for a transaction by the card, the server compares the received action counter value with the latest value stored, incremented by the number of actions contained in the previous request for actions and, operates on the basis of this comparison.--

IN THE CLAIMS:

Kindly amend the following claims.

1. (Amended) A method of monitoring an execution of a request for actions transmitted by a server to a card via a terminal, [the] said card including an action counter, [characterised in that it includes] comprising the following steps;

a) on the sending by the server of a message including a request comprising one or more actions to be implemented by the card, the server stores the number [n] of actions in the request;

b) on reception of the message, the card successively executes the action or actions in the request whilst incrementing its action counter between each action if the action is properly executed and refusing this action and [the] successive actions if the action has not been correctly executed, without incrementing its counter; and

c) the variation between the value in the card and the one stored in the server are compared and [it is determined] a determination is made that the last x actions [(commands)] are not executed if the result of the comparison has a difference of x.

2. (Amended) A method according to Claim 1, [characterised in that] wherein, in order to compare the variation between the value in the card and the one stored in the server, the card transmits to the server the current value of its counter before and after execution of the action [command].

3. (Amended) A method according to Claim 1, [characterised in that] wherein, in order [the] to compare the variation between the value in the card and the one stored in the server, the card calculates the value of the variation in its counter following the execution of the action [command] and transmits it to the server.

4. (Amended) A method according to [one of Claims 2 or 3, characterised in that] Claim 3, wherein the card transmits [the] said values in protected form.

5. (Amended) A method of exchange of messages according to Claim 1, [characterised in that] wherein the value of the card action counter is transmitted in real time[, that is to say] during the current transaction.

6. (Amended) A method of exchanging messages according to Claim 5, [characterised in that] wherein the value of the card action counter is transmitted to the server by means of a message acknowledging the current transaction in the card.

7. (Amended) A method of exchanging messages according to Claim 1, [characterised in that] wherein the value of the card action counter is transmitted in non-real time.

8. (Amended) A method of exchanging messages according to Claim 7, [characterised in that] wherein the value of the card action counter is transmitted to the server by means of a message of a new transaction request by the card for the server.

9. (Amended) A method of exchanging messages according to Claim 7, [characterised in that] wherein the value of the card action counter is transmitted by means of an information message sent by the card to the server.

Cancel claim 10.

Add the following new claims:

--11. A method according to Claim 2, wherein the card transmits said values in protected form.

12. A microprocessor card, comprising:

an application which executes actions in response to a transaction request received from a server;

an action counter; and

a counter manager which increments said action counter upon proper execution of each action and inhibits the incrementing of the counter for any action which is not properly executed and all successive actions in a transaction, and which transmits the value of said counter to the server.

13. The microprocessor card of claim 12, wherein said value is transmitted in a protected form.

14. The microprocessor card of claim 12, wherein said value is transmitted in real time during the transaction.

15. The microprocessor card of claim 14 wherein said value is transmitted together with an acknowledgment message pertaining to a current transaction.

16. The microprocessor card of claim 12 wherein said value is transmitted in non-real time after the transaction has terminated.

17. The microprocessor card of claim 16 wherein said value is transmitted together with a message sent by the card requesting a new transaction.--

REMARKS

Entry of the foregoing amendments is respectfully requested. These amendments are intended to further clarify the language of the claims and specification.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: January 29, 2001

A METHOD OF CONTROLLING THE EXECUTION OF A REQUEST FOR ACTIONS TRANSMITTED BY A SERVER TO A CHIP CARD VIA A TERMINAL

The present invention relates to systems for exchanges of messages between an application server and chip cards using a communication network. It applies to exchanges taking place through telecommunication networks, switched telephone networks, cellular networks or the Internet.

Generally the messages exchanged between an application server and the corresponding application in a chip card pass through intermediate equipment which will be referred to as a terminal hereinafter. The chip card of a user co-operates with the terminal to allow the exchanges.

Where the network used is a telephony network, the terminal is a telecommunications terminal. Where the network used is a computer network, the terminal is

data processing equipment of the computer type equipped with an interface for reading/writing to chip cards.

A server under the control of a card-issuing organisation wishing to effect a protected action in a chip card (or in an application of the said card) via a telephone network uses cryptographic certificates for ensuring the security of the exchanges.

However, in the event of the loss of a message during the transmission or execution or in the case of an attempted fraud, the re-synchronisation of the server/card messages can pose security problems.

Where the terminal is a dedicated protected terminal under the control of the issuing body (for example an automatic note dispenser AND under the control of a bank), the loss of a message is compensated for by synchronisation messages using both the software of the server and the software of the dedicated terminal. The dedicated terminal is protected either physically (AND) or contains inside it an SAM (Secure Authentication Module), and in all cases is closely monitored by the issuing organisation.

If the terminal used is not a dedicated protected terminal (for example a GSM telephone, PC on the Internet, etc), the synchronisation mechanisms cannot be based on the security of the terminal, because the latter cannot be monitored by the issuer.

In fact it is important to be able to re-synchronise the source of the messages and the chip card in the event of any transmission problem on the

network. This problem has been posed in terms of security vis-à-vis operators and service providers.

At the present time there is no system designed to ensure synchronisation between the card and server, in cases where during a current transaction, consequently accepted by the card, the server profits from the connection to send a message containing one or more actions to be implemented by the card, these actions being able, for example, to be a re-charging of units of value or parameters (monetary or other) or a loading of a new application.

In fact, provision is made, in the more general context of multi-application cards, for messages to be sent when the user has made a transaction request in order to send commands for actions to be undertaken during the running of the application for the current transaction.

Such messages will for example make it possible to control an electric purse recharging in the case of an electronic purse application, or to modify banking parameters of the bank application, or the loading of a new application into the card.

It is clear that, in this situation, the server will not be informed where the said message is lost.

In other words, performing protected actions on a non-dedicated terminal is feasible today but requires either high user constraints (cards or applications blocked if the security action has not ended), or risks of loss of information (for example loss of a transaction for recharging an electronic purse).

The purpose of the invention is that the server can detect failures in execution of one or more actions or commands, linked to a loss of messages between the server and chip card or to failure to execute actions in the card, the said messages having been transmitted to the card, possibly during a current transaction, in order to inform the server thereof so that the latter determines what are the last actions or commands not executed by the card.

According to a procedure pre-established in accordance with the action or actions not implemented, the server can for example send back the message containing the said action or actions and allow their execution.

To this end, the object of the invention is particularly a method of monitoring an execution of a request for actions transmitted by a server to a card via a terminal, the said card including an action counter, characterised in that it includes the following steps;

a) on the sending by the server of a message including a request comprising one or more actions to be implemented by the card, the server stores the number n of actions in the request;

b) on reception of the message, the card successively executes the action or actions in the request whilst incrementing its action counter between each action if the action is properly executed and refusing this action and the successive actions if the

action has not been correctly executed without incrementing its counter;

c) the variation between the value in the card and the one stored in the server are compared and it is determined that the last x actions (commands) are not executed if the result of the comparison has a difference of x.

The incrementation of the action counter corresponds to the number of actions correctly executed.

The number x is equal to 0 if all the actions are correctly executed; this number x can therefore vary from 1 to n if the last or all the actions have failed.

To compare the variation between the value in the card and the one stored in the server, the card transmits to the server the current value of its counter before and after execution of the action command.

To compare the variation between the value in the card and the one stored in the server, the card calculates the value of the variation of its counter following the execution of the action command and transmits it to the server.

According to another characteristic, any exchange of the value of the action counter of the card is effected systematically in a protected manner.

To this end, the last value of the action counter of the card is transmitted with a cryptogram whose calculation involves the said last value.

According to another characteristic the current last value of the action counter in the card is transmitted to the server in real time, that is to say during the current transaction.

According to one example the value can be transmitted by means of the message acknowledging the current transaction in the card.

According to another characteristic the value of the card action counter is transmitted to the server in non real time.

According to one example the value of the action counter can be transmitted by means of a message of a new request for a transaction by the card by the server.

According to another example the value of the card action counter is transmitted by means of an information method sent from the card to the server.

Another object of the invention is a card for implementing the aforementioned method including a counter and means of managing this counter, characterised in that the said management means are able to increment the said action counter between each action if the action is correctly executed and not to increment it for this action nor for the following actions if this action has not been executed.

Other characteristics and advantages of the present invention will emerge from the reading of the following description given below by way of non-limited example and with regard to the drawings in which:

- Figure 1 illustrates message exchanges between server and chip card according to the invention,

- Figure 2 illustrates in detail message exchanges between server and chip card in the case of the loss of a message,

- Figure 3 illustrates another case of the loss of a message.

Action request means a message containing a set of n commands, n of course being able to be equal to 1.

For a better understanding of the remainder of the description, reference can be made to the diagram in Figure 1.

Throughout the remainder, the case where the server 2 profits from a current transaction in a card 1 in order to send it a request containing one or more actions which the card is to execute has been taken as an example.

Naturally in this case an action request will be sent with the response to the current transaction if the said transaction requires a response. If such is not the case, a response is created containing solely the action request. The terminal which is in communication with the server receives the message corresponding to this response, and removes the envelope from this message in order to transmit the actions to the card.

An action request can include several actions to be undertaken by the card, that is to say, as stated at the beginning of the description, a set of n commands.

By way of example an action request can be a request to change one or more parameters in an application program or the loading of a new application or the charging of units of value.

The change of a parameter corresponds to an action from the card which is an operation of erasure and writing at a predetermined address.

The change of several parameters corresponds to as many erasure and writing operations at distinct addresses as there are parameters and consequently to as many actions to be undertaken as there are parameters to be changed.

Details will now be given of what occurs on the card side and the server side.

Card side:

The card 1 increments, after each correctly performed action, the action counter CA as soon as it receives from the server one or more actions to be undertaken and as soon as it has been able to successfully execute each of these actions.

The value of the counter is sent back to the server, for example each time the card sends a message to the server (message 3 or message 4 in Figure 1).

The value of the counter can be sent back to the server 2 essentially at the time of the following actions:

- when there is a transaction acknowledgement (if during a transaction an acknowledgement message is sent back to the server the value of the action counter can be put in this acknowledgement) (example: message 3),

- when there is a transaction request or card authentication request to the server (example: message 4),

- in the case of bank cards or electronic purses,

- every past transaction is stored in each terminal 3,

- the stored transaction is sent back to the server so that the server can trigger the process of paying the merchant with whom the transaction took place, the action counter CA can be sent back with this transaction.

Thus the value of the content of the action counter is always sent back to the server either in real time when this is done at the time of acknowledgement or in non real time when there is a new transaction request or when a transaction storage is sent back.

Server side:

For each card containing an application which is dedicated to it having a current action request, the server must store:

- the identification number of the application,
- the current value of the action counter,
- the list of current actions for this card.

Thus the server to which there belongs an application placed in a multi-application chip card can, during any transaction requested by the card, demand an action such as a recharging of units, or a loading of a program or a loading of new parameters for a program resident in the card.

The server can thus send actions to the card by a script mechanism which cannot be interpreted by the terminal 3, which is situated between the server and the card in order to provide communication. The terminal 3 transmits the message or messages received in the script to the card in a transparent manner.

Details will now be given of all the processing in the case where the sending back of the content of the action counter takes place in real time and in the case where everything occurs correctly, that is to say in the case where there is no loss of message and where the execution by the card has taken place correctly.

Reference can be made to the particular embodiment illustrated by the diagram in Figure 1 to give a better understanding.

- At time dti the bearer requests, via his terminal 3, a transaction (a payment or another transaction): message 1.

- The card prepares the transaction and a cryptogram, that is to say the authentication data, designated hereafter as MAC, and transmits to the terminal.

Associated with this transaction, the banking application joins the current value of CA of its action counter protected by the cryptogram.

- The terminal sends back the transaction to the bank server.

In practical terms, the card sends a transaction request message containing the data MAC1 and the value

of the action counter CA, and the identification of the requested transaction.

The server verifies the authentication data for the card MAC1 and processes the transaction. The server can at this moment perform an action in the card application.

In a particular example, it may be a case of the loading of a monetary parameter into the card, but, as stated, other actions of the electronic purse recharging type are also possible.

- For this purpose, the server will prepare one or more parameter loading commands contained in an information field in an action referred to as script 1, and the security authentication data MAC2.

- The action request is sent by means of a message 2 which can contain the response to the current transaction if such a response is provided for the application concerned.

At the time of the sending of script 1 to the card, the server stores this script 1 in a database, associating therewith the data relating to the card, as well as the current value CA of the action counter of the card (sent from the card to the server during the transaction request). This information will make it possible to effect the server-card synchronisation.

- The card, which receives the commands one by one from script 1, verifies the cryptogram MAC2, and atomically (that is to say on a single occasion and indivisibly) performs action by action in the list of script 1 and increments the content CA of the counter

after each action if this has occurred correctly. When an action has occurred incorrectly, the action counter is not incremented and the other actions are not accepted.

- In order to send to the server the new value CA' of the action counter CA of the card, several schemes are possible:

  - sending back during a message acknowledging the current transaction, that is to say in real time (corresponds to the message 3 of the current transaction);

  - sending back the value of CA' during the next transaction (corresponds to the message 4 occurring at time dtj);

  - at any time, that is to say when the card sends information to the server.

- In the case of the example described, the card sends a protected acknowledgement to the server including the content CA' in real time. This can then compare the value returned by the acknowledgement with the value stored in its base.

If the value of CA' = CA+n, n being the number of actions of the script 1, this proves that the script 1 has been run correctly in the card. The server can then erase this script in the database.

A description will now be given, in relation to Figure 2, taking the same example, of what happens when a cutoff or a loss of action request message (message 2) occurs.

In this case, the command script 1 has not arrived in the card. The server will have to re-synchronise itself. The server is informed of this situation since according to this example it has not received an acknowledgement.

Where the server is not awaiting an acknowledgement, it is informed of when it receives the last of the card action counter, that is to say for example at the next transaction.

In fact, during the authentication of the card by the server (verification MAC1), the server identifies that this card has not received script 1 (or that script 1 has not been effected correctly in the card) by means of the value of CA' of the action counter which is sent back to the server and compared with the value of CA stored in the server.

If CA' is less than CA and not equal, this means that the last action or actions have not been performed correctly.

In this case the server updates its database DB, erasing the value of CA in order to put in the value of CA'. The server is once again synchronised and can re-initiate the last action or actions not executed by the card.

A description will now be given, in relation to Figure 3, still repeating the same example, of what happens when a cutoff occurs during the acknowledgement message.

This case can be envisaged only where an acknowledgement message is provided with the

application. However, the same problem can occur when the action counter is sent back at the time of a request for a new transaction, or the sending of an information message.

In this case, at the time of the new transaction request, the current value of the action counter of the card CA' = CA+n is sent back.

The server compares this value CA' with its last stored value, that is to say CA. As CA' = CA+n, the server knows that the last n actions have indeed been undertaken and stores the new value of the action counter, that is to say CA+n, in order to be synchronised with the card.

CLAIMS

1. A method of monitoring an execution of a request for actions transmitted by a server to a card via a terminal, the said card including an action counter, characterised in that it includes the following steps;

a) on the sending by the server of a message including a request comprising one or more actions to be implemented by the card, the server stores the number n of actions in the request;

b) on reception of the message, the card successively executes the action or actions in the request whilst incrementing its action counter between each action if the action is properly executed and refusing this action and the successive actions if the action has not been correctly executed without incrementing its counter;

c) the variation between the value in the card and the one stored in the server are compared and it is determined that the last x actions (commands) are not executed if the result of the comparison has a difference of x.

2. A method according to Claim 1, characterised in that, in order to compare the variation between the value in the card and the one stored in the server, the card transmits to the server the current value of its counter before and after execution of the action command.

3. A method according to Claim 1, characterised in that, in order the compare the variation between the value in the card and the one stored in the server, the card calculates the value of the variation in its counter following the execution of the action command and transmits it to the server.

4. A method according to one of Claims 2 or 3, characterised in that the card transmits the said values in protected form.

5. A method of exchange of messages according to Claim 1, characterised in that the value of the card action counter is transmitted in real time, that is to say during the current transaction.

6. A method of exchanging messages according to Claim 5, characterised in that the value of the card action counter is transmitted to the server by means of a message acknowledging the current transaction in the card.

7. A method of exchanging messages according to Claim 1, characterised in that the value of the card action counter is transmitted in non real time.

8. A method of exchanging messages according to Claim 7, characterised in that the value of the card action counter is transmitted to the server by means of a message of a new transaction request by the card for the server.

9. A method of exchanging messages according to Claim 7, characterised in that the value of the card action counter is transmitted by means of an information message sent by the card to the server.

10. A card for implementing the method according to one of the preceding claims, having a counter and means for managing this counter, characterised in that the said management means are able to increment the said action counter between each action, if the action has been correctly executed, and not to increment it for this action nor for the following actions if this action has not been executed.

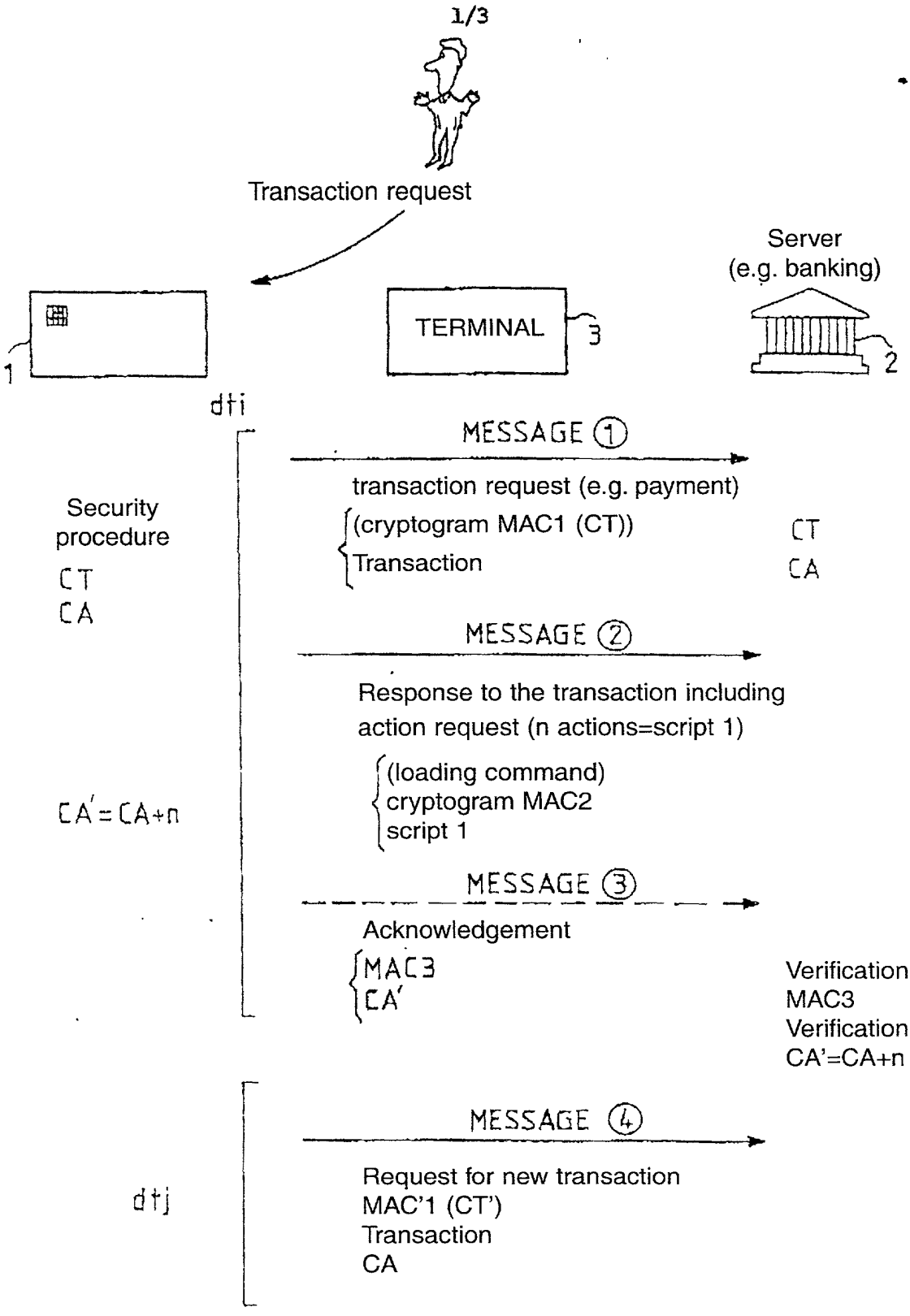
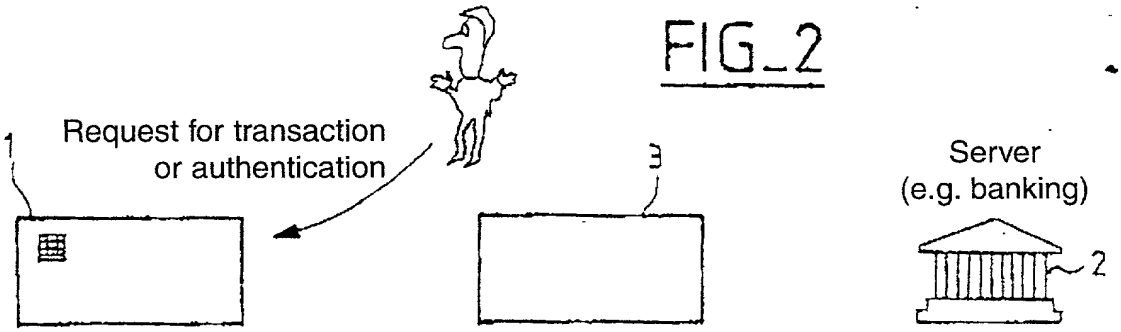

Transaction request
Server
(e.g. banking)
TERMINAL
3
1
2
dti
MESSAGE ①
transaction request (e.g. payment)
(cryptogram MAC1 (CT))
Transaction
CT
CA
Security
procedure
CT
CA
MESSAGE ②
Response to the transaction including
action request (n actions=script 1)
(loading command)
cryptogram MAC2
script 1
CA'=CA+n
MESSAGE ③
Acknowledgement
MAC3
CA'
Verification
MAC3
Verification
CA'=CA+n
MESSAGE ④
Request for new transaction
MAC'1 (CT')
Transaction
CA
dtj

FIG_1

FIG_2



Application
- Calculation of card authentication data MAC1.
Reading of action counter CA

MESSAGE ①

Transaction request
- MAC1
- CA
- Banking transaction

- Verification MAC1
- Performs the transaction
- Calculation of server authentication data MAC2
- Preparation of command for changing parameter of script 1
- Storage of CA and script 1 in DB server

E.g. line cut off

MESSAGE ②

Response to transaction including action request (script 1)

{loading command
MAC2, script 1)

MESSAGE ③

New transaction request

{- MAC1, CA
- Banking transaction

Application
- Calculation of card authentication data MAC1
- Reading of action counter CA

- Verification of MAC1
- Verification of CA_{card} = CA_{server} ⇨ cancels last transaction
- Calculation of MAC2
- Preparation of new script 2
Storage CA' and script 2 in DB server

MESSAGE ④

Response to transaction including action request (script 2)

{Loading command
MAC 2, script 2

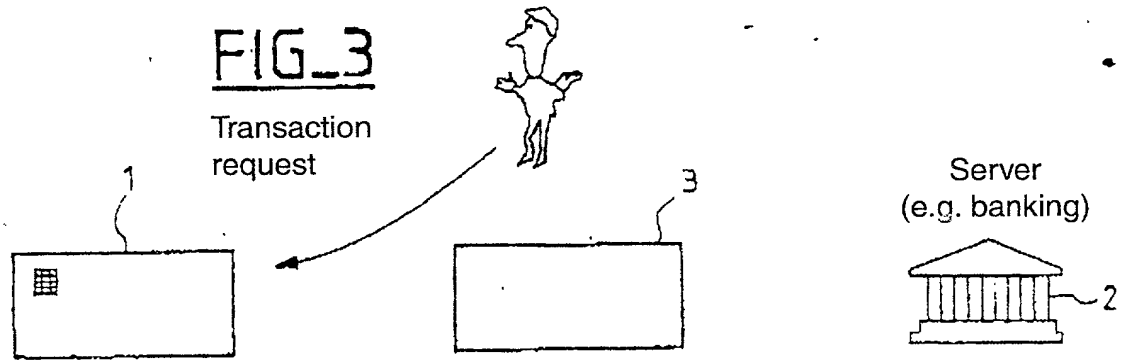
- Verification of MC2
- If MAC2 OK then effect script 2#
- If script 1 OK, incrementation CA=CA+1
- Calculation of acknowledgement MAC3

MESSAGE ⑤

Acknowledgement
MAC 3, CA+1

- Verification MAC 3
- Verification CA'=CA+1
- Erasure of DB

FIG_3



Application
- Calculation of card authentication data MAC1.
- Reader for action counter CA

MESSAGE (1)

Transaction request
- MAC1
- CA
- Banking transaction

- Verification of MAC1
- Effects transaction
- Calculation of server authentication data MAC2
- Preparation of change in parameter command script 1
- Storage of CA and script in DB server

MESSAGE (2)

Response to transaction including action request (script 1)
{Loading command
MAC2, script 1

- Verification of MAC2
- if MAC 2 OK then effect script 1
- if script 1 OK incrementation CA'=CA+1
- Calculation of acknowledgement MAC3

MESSAGE (3) (e.g. line cutoff)

Acknowledgement

MESSAGE (4)

New action request
- MAC1, CA'
- Banking transaction

- Verification of MAC1
- Verification
- CA' $_{card}$=CA+n last transaction OK
- Effects current transaction
- Calculation MAC2
- Preparation new script 2
- Storage CA' in script 2 in DB server

Application
- Calculation of card authentication data MAC1
- Reading of action counter CA'=CA+n

MESSAGE (5)

Response to transaction including action request (script 2)
{Loading command
MAC2, script 2

- Verification MC2
- if MAC2 OK then effects script 2
- if script 1 OK, incrementation CA'=CA'+1
- Calculation of acknowledgement MAC3

MESSAGE (6)

Acknowledgement
MAC3, CA'

- Verification MAC3
- Verification of CA'=CA'+1
- Erasure of DB

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY **(Includes Reference to Provisional and PCT International Applications)**	Attorney's Docket No.

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR CONTROLLING THE EXECUTION OF A REQUEST FOR ACTION TRANSMITTED BY A SERVER TO A CHIP CARD VIA A TERMINAL.

the specification of which (check only one item below):

- is attached hereto.
- was filed as United States application
  Number _____
  on _____
  and was amended
  on _____ (if applicable).
- was filed as PCT international application
  Number PCT/FR 99/01826
  on JULY 26TH 1999.
  and was amended
  on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §119
PCT.	WO 00/07153	10-02-2000	_ Yes _ No
FRANCE	98 09575.	24-07-1998	_ Yes _ No
			_ Yes _ No
			_ Yes _ No
			_ Yes _ No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

_____ _____
(Application Number) (Filing Date)

_____ _____
(Application Number) (Filing Date)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) **(Includes Reference to Provisional and PCT International Applications)**	Attorney's Docket No.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States applications(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations §1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. §120:

U.S. APPLICATIONS		**STATUS *(check one)***		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED

PCT APPLICATIONS DESIGNATING THE U.S.					
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)			

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	R. Danny Huntington	27,903	Gerald F. Swiss	30,113
Robert S. Swecker	19,885	Eric H. Weisblatt	30,505	Michael J. Ure	33,089
Platon N. Mandros	22,124	James W. Peterson	26,057	Charles F. Wieland III	33,096
Benton S. Duffett, Jr.	22,030	Teresa Stanek Rea	30,427	Bruce T. Wieder	33,815
Norman H. Stepno	22,716	Robert E. Krebs	25,885	Todd R. Walters	34,040
Ronald L. Grudziecki	24,970	William C. Rowland	30,888	Ronni S. Jillions	31,979
Frederick G. Michaud, Jr.	26,003	T. Gene Dillahunty	25,423	Harold R Brown III	36,341
Alan E. Kopecki	25,813	Patrick C. Keane	32,858	Allen R. Baum	36,086
Regis E. Slutter	26,999	Bruce J. Boggs, Jr.	32,344	Steven M. du Bois	35,023
Samuel C. Miller, III	27,360	William H. Benz	25,952	Brian P. O'Shaughnessy	32,747
Robert G. Mukai	28,531	Peter K. Skiff	31,917	Kenneth B. Leffler	36,075
George A. Hovanec, Jr.	28,223	Richard J. McGrath	29,195	Fred W. Hathaway	32,236
James A. LaBarre	28,632	Matthew L. Schneider	32,814		
E. Joseph Gess	28,510	Michael G. Savage	32,596		

21839

and: _____

Address all correspondence to:

21839

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and PCT International Applications)	Attorney's Docket No.

FULL NAME OF SOLE OR FIRST INVENTOR	SIGNATURE	DATE
DOMINIQUE ARCHER		3/12/2000
RESIDENCE	CITIZENSHIP	
69 avenue des oliviers		
POST OFFICE ADDRESS		
69 Avenue des oliviers 83740 LA CADIÈRE.		FRX
FULL NAME OF SECOND JOINT INVENTOR, IF ANY	SIGNATURE	DATE
Patrick Imbert		11/12/2000
RESIDENCE	CITIZENSHIP	
35 rue de la Sauge		
POST OFFICE ADDRESS		
35 rue de la Sauge Parc des 7 collines 13011 Marseille		FRX
FULL NAME OF THIRD JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE	CITIZENSHIP	
POST OFFICE ADDRESS		